Radiation Detection Information Barriers

James Fuller
Pacific Northwest National Laboratory

A radiation detection system information barrier consists of procedures and technology that prevent the release of sensitive information during a joint inspection of a sensitive item, and it provides confidence that the measurement system functions exactly as designed and constructed. The U.S. has been studying information barriers in a coordinated fashion since January 1999 and has briefed the results of our studies to Russian counterparts during several official interactions.

The basic functional requirements for any information barrier are that (1) the host must be assured that his classified information is protected from disclosure to the monitoring party, and (2) the monitor must be confident that the integrated inspection system measures, processes, and presents the conclusion in an accurate and reproducible manner. It is to be emphasized, however, that the protection of host country classified information is paramount.

In the U.S. during the first part of 1999, a Joint DoD (Department of Defense)/DOE (Department of Energy) Information Barrier Working Group (IBWG) was established to reach consensus on the fundamental design guidelines for information barriers. Guidance was developed around nine design elements. A listing of these elements and summary of the guidance is provided below.

(1) Equipment Supply and Certification. The best way for the host country to be assured that its classified information is protected is for the host country to supply the monitoring equipment and to certify that it meets its own security requirements. This being then case, then most of remaining design guidance must be focused providing confidence to monitors about measurement system integrity.

(2) Central Processing Units. CPUs need to conform to a "trusted processor" design principles, having extraneous functionality eliminated.

(3) Non-CPU Equipment. Non-CPU systems need to be considered on a case-by-case basis but must also be trusted and inspectable.

(4) Procedural Issues. The measurement equipment must be designed and configured to avoid deduction of classified information by simply observing system operation. This needs to be evaluated on a case-by-case basis, but certainly includes the use of fixed (not real) counting times.

(5) Electronic Emanation Considerations. Equipment should be evaluated for emanations according to the information security standards and practices acceptable to the host. But also, the monitoring party will have to perform system-level assessments to assure that radio control of the results is not possible, and the monitoring party might

need to demand more rigorous emanation protection than that found to be adequate by the host for his information protection concerns.

(6) Multiple/Intermediate Barriers. If intermediate barriers can be employed without compromising measurement system functionality assurances, then it may be desirable to do so.

(7) Software, Firmware, and CPU Operating Systems. The software at every level must be completely inspectable and documented; the amount of code must be minimized; and complex operating systems and compilers avoided.

(8) Inputs and Outputs. All I/O must have a dedicated and well-understood function, with no extraneous ports/devices; simple displays should be used for yes/no type output results; peripherals and bus structures should be avoided.

(9) Measurement System Authentication and Repair. Multiple copies of host-provided equipment should be maintained under jointly secured storage, with the monitoring party having the right to select one for inspection and one for replacement in a broken subsystem. Software should be similarly supplied on demand.

The United States assessment is that there are a limited number of basic design criteria that need to be considered in developing a radiation detection and monitoring system integrated with an information barrier. It is our assessment that there are procedural and technological solutions available to assure the protection of host-country classified information and to provide monitoring party confidence in system integrity. It is also the assessment by the United States that joint development of information barriers provides the greatest degree of trust and transparency. The system demonstrated at Los Alamos in August 2000 incorporated examples of all the design elements described above.

The best way for the monitor to gain confidence about the integrity of a measurement system integrated with an information barrier is to have the right, with the assistance of the host country, to authenticate the installed system. Three tools to carry out authentication are (1) random selection of host-supplied modular equipment; (2) use of trusted, unclassified calibration sources; and (3) thorough joint inspection using detailed design documentation.